

The diagram illustrates a cryptographic device 100, enclosed in a dashed box. The process begins with an input X entering an INPUT UNIT (10). The output of the input unit flows into a series of processing units:

- FIRST UNIT (1):** Performs a MODULO OPERATION. It receives a feedback signal Z_1 from the output unit.
- SECOND UNIT (2):** Performs a NIBBLE SWAP. It receives a feedback signal Z_2 from the output unit and a key stream signal W_1 from the first unit.
- THIRD UNIT (3):** Performs a CUSTOM OPERATION. It receives a feedback signal Z_3 from the output unit and a key stream signal W_2 from the second unit.
- FOURTH UNIT (4):** Performs a NIBBLE SWAP. It receives a feedback signal Z_4 from the output unit and a key stream signal W_3 from the third unit.
- FIFTH UNIT (5):** Performs a MODULO OPERATION. It receives a feedback signal Z_5 from the output unit and a key stream signal W_4 from the fourth unit.
- SIXTH UNIT (6):** Performs a NON LINEAR MODULO OPERATION. It receives a feedback signal Z_6 from the output unit and a key stream signal W_5 from the fifth unit.
- SEVENTH UNIT (7):** Performs a NON-INVERTIBLE OPERATION. It receives a feedback signal Z_7 from the output unit and a key stream signal W_6 from the sixth unit.
- EIGHTH UNIT (8):** Performs a MODULO OPERATION. It receives a feedback signal Z_8 from the output unit and a key stream signal W_7 from the seventh unit.

The output of the eighth unit flows into the OUTPUT UNIT (11), which produces the final output Y . A feedback loop connects the output Y back to the input of the first unit, passing through a series of intermediate signals Z_1 through Z_8 . Additionally, a KEY SCHEDULER UNIT (9) receives an external input Z_9 and provides the key stream signals W_1 through W_8 to the corresponding processing units.

FIG. 1

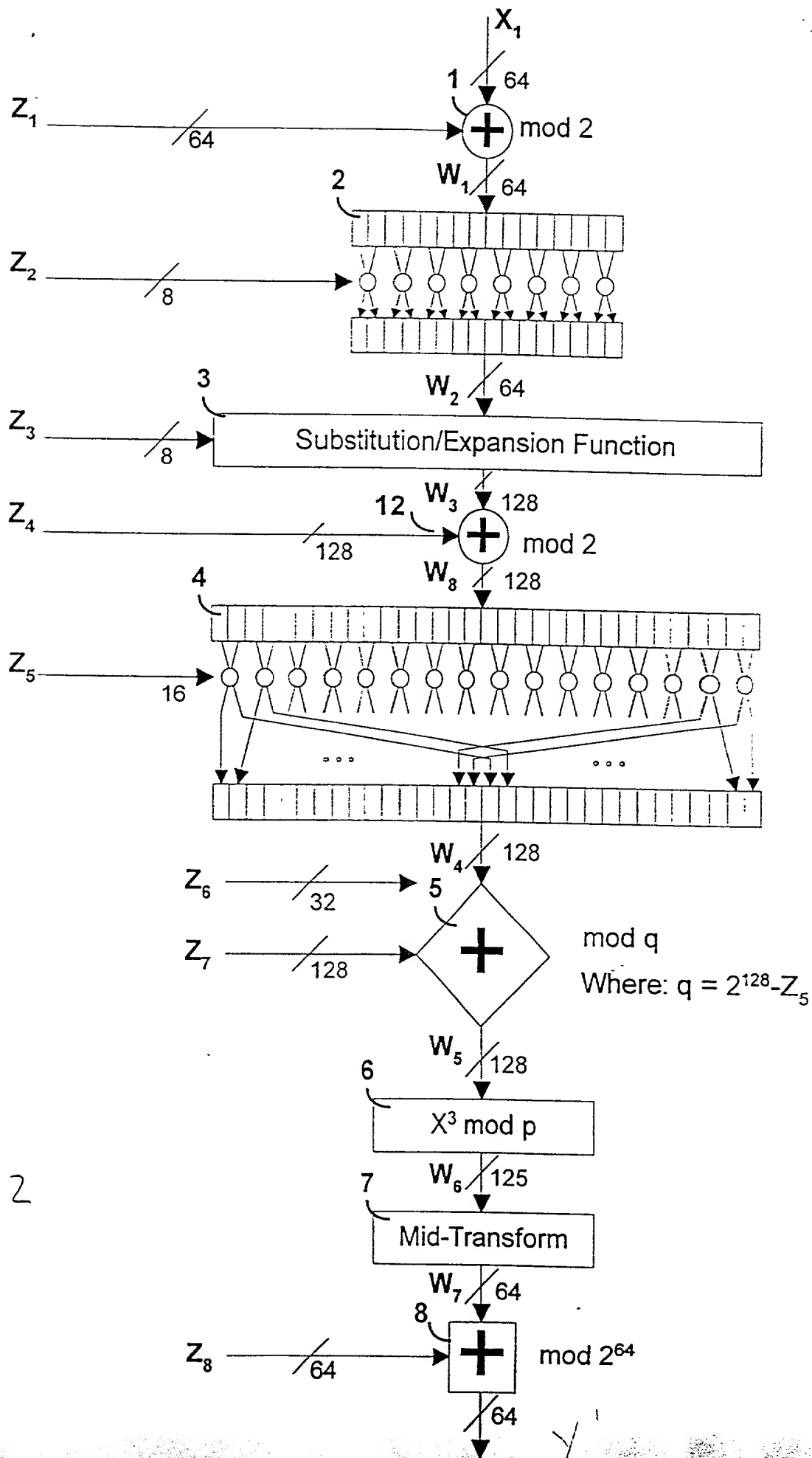


FIGURE 2

10699794660

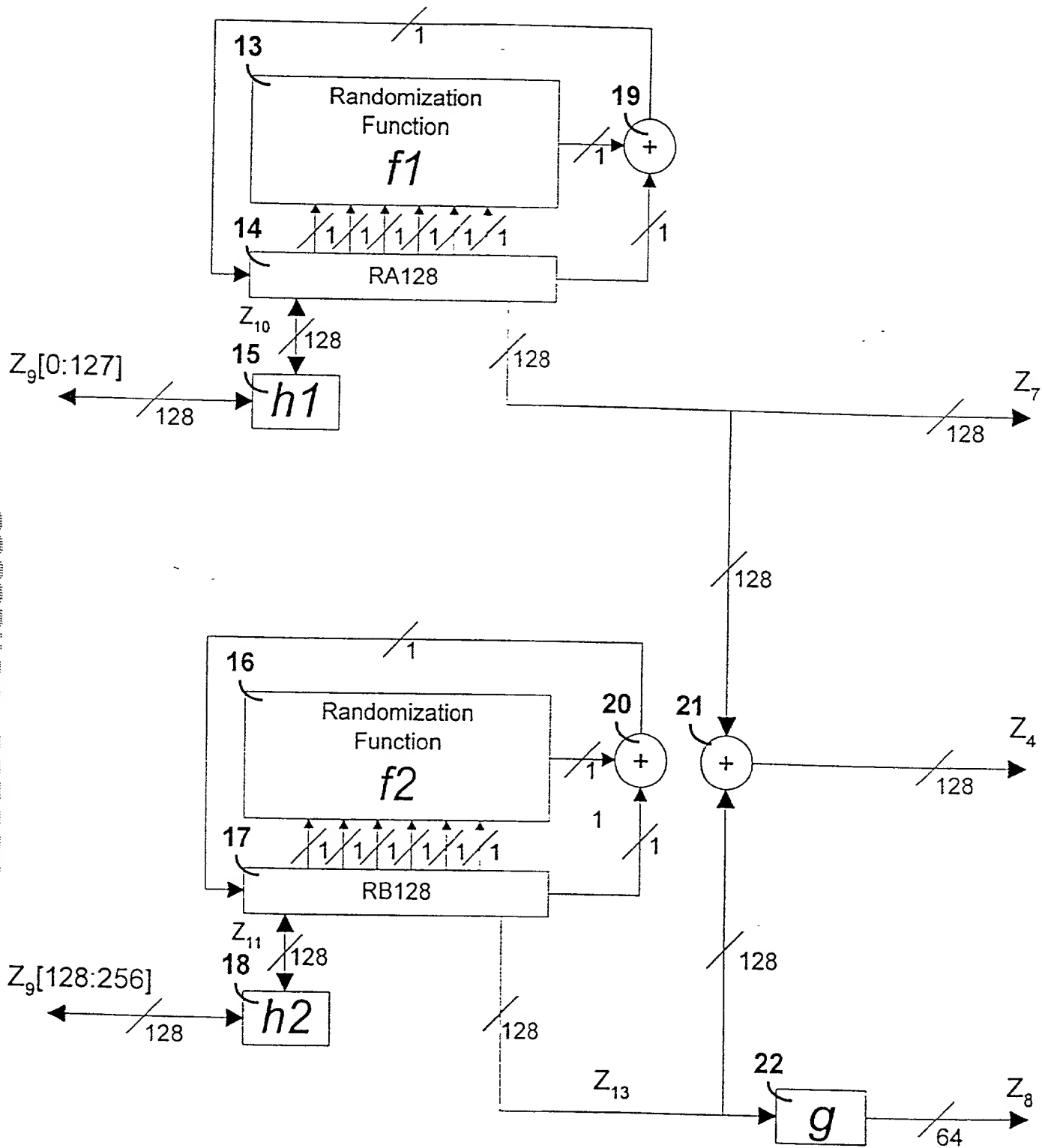


FIGURE 3

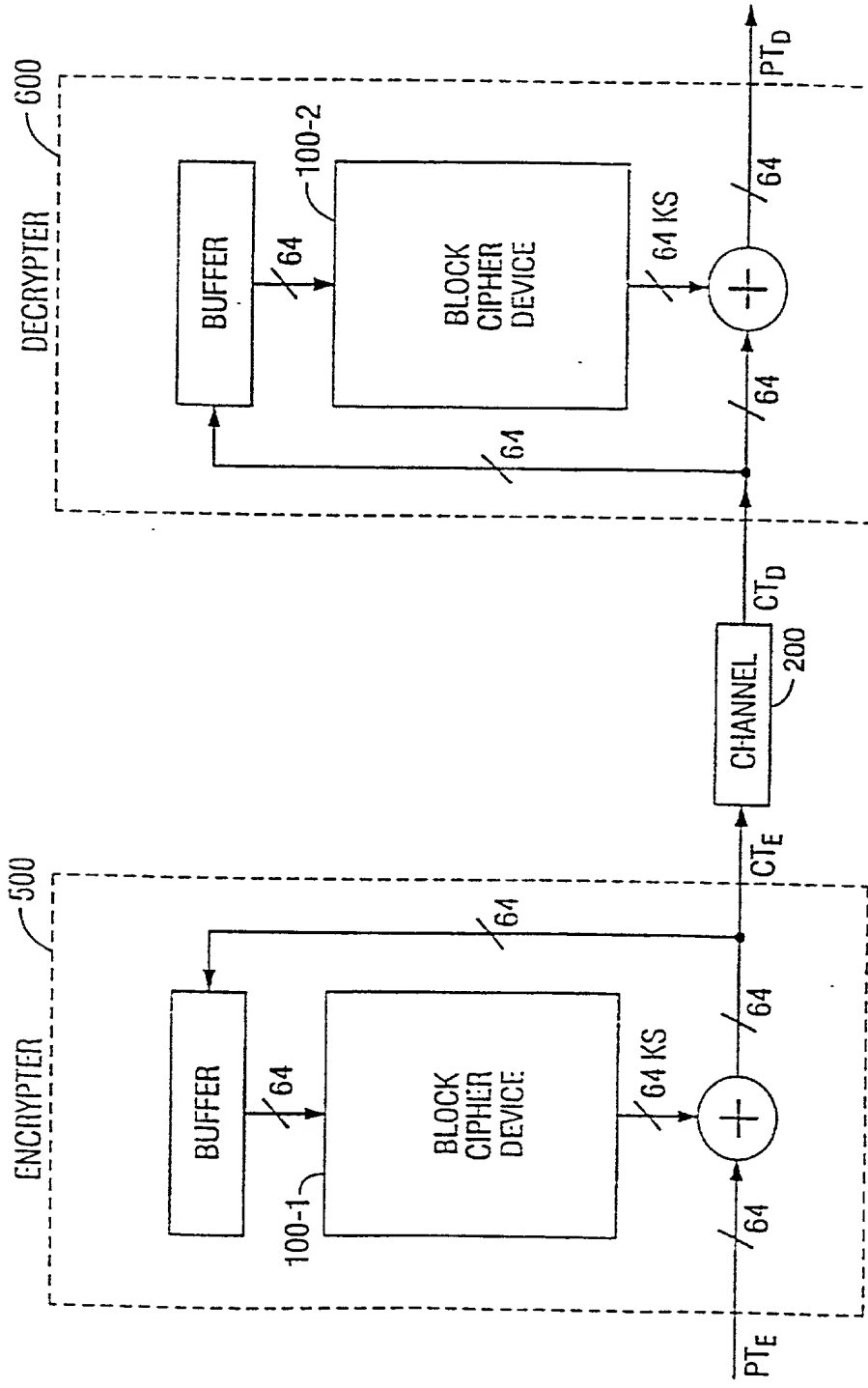


FIG. 4

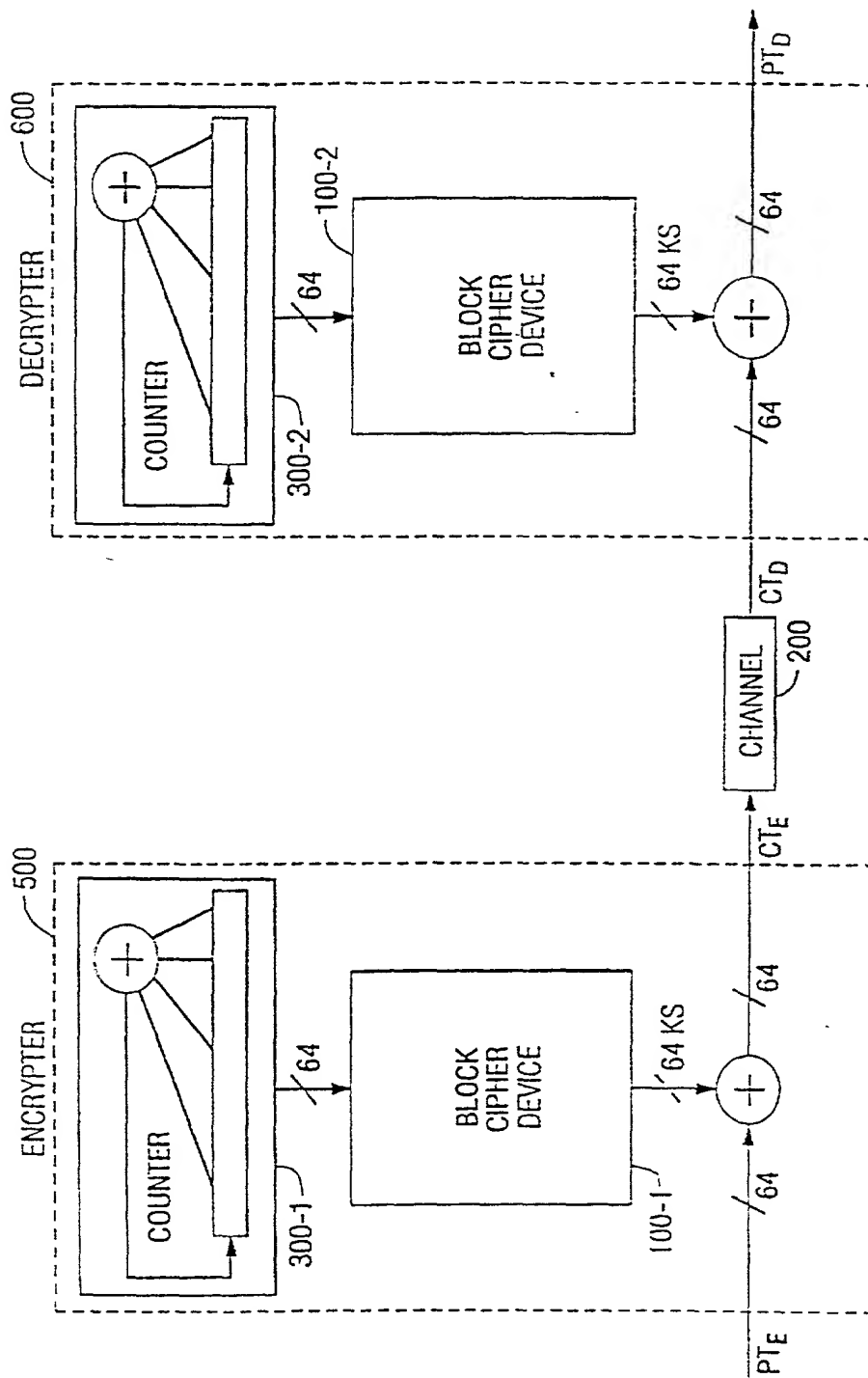


FIG. 5

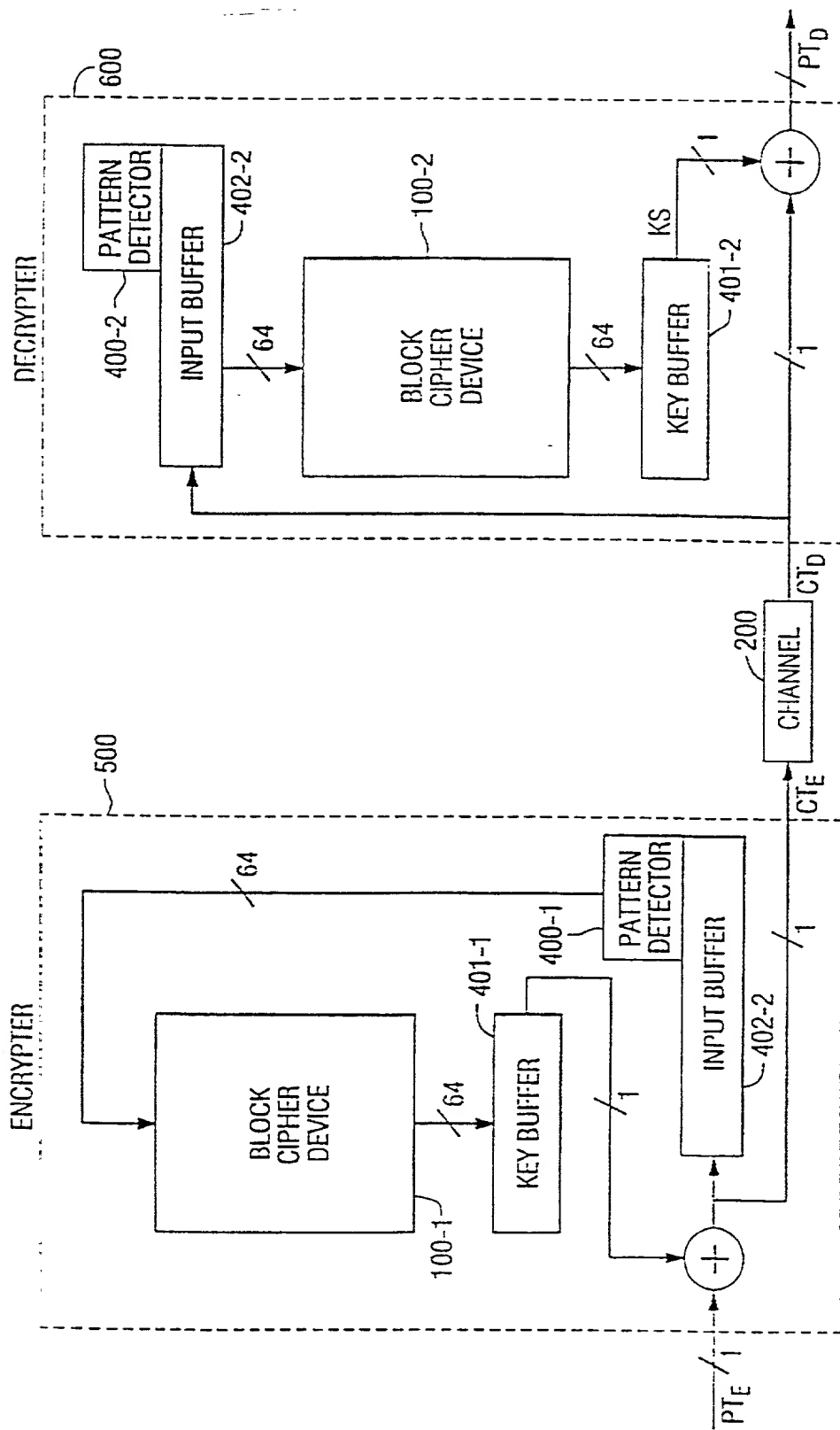


FIG. 6